Graphical User Authentication

LALZIRTIRA
(211CS2058)

under the guidance of
Prof. SANJAY KUMAR JENA

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela – 769 008, India.

May 2013.

Graphical User Authentication

A thesis submitted

in partial fulfillment of the requirements

for the degree of

Master of Technology

in

COMPUTER SCIENCE and ENGINEERING

by

LALZIRTIRA

(Roll 211CS2058)

under the supervision of

Prof. SANJAY KUMAR JENA

Department of Computer Science and Engineering

National Institute of Technology Rourkela

Rourkela – 769 008, India

Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769 008, India. www.nitrkl.ac.in

Dr. Sanjay Kumar Jena
Professor,
Department of Computer Science & Engineering.

May 31, 2013

Certificate

This is to certify that the work in the thesis entitled ***"Graphical User Authentication"*** by ***Lalzirtira***, bearing roll number 211CS2058, is a record of an original research work carried out by him under my supervision and guidance in partial fulfillment of the requirements for the award of the degree of ***Master of Technology*** in ***Computer Science and Engineering***. Neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere.

Prof. Sanjay Kumar Jena

Acknowledgment

GLORY TO GOD IN THE HIGHEST. First and foremost, I give thanks to Almighty God for all HIS blessings that he bestowed upon me without which I won't be where I am today.

I would like to express my sincere gratitude to my advisor and guide, Prof. S.K Jena for the continuous support of my thesis study, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor. I also am indebted to all the professors, co-researchers, batch mates and friends at National Institute of Technology, Rourkela for their active or hidden cooperation.

I thank all the members of the Department of Computer Science and Engineering, and the Institute, who helped me by providing the necessary resources, and in various other ways, in the completion of my work.

Last but not the least, I would like to thank my friends and families, who always encouraged me at times of difficulties. I especially thank my mother and my father for bringing me into this world and for all their love and support throughout my life. Their unending love and their sleepless prayers are the only things that brought me to this day.

Lalzirtira

I will instruct thee and teach thee in the way which thou shalt go: I will guide thee with mine eye.

Psalm 32:8

Abstract

Today, authentication technology is the main measure to guarantee information security, and the most common and convenient authentication method in use is the alphanumeric password. However, their inherent defects led to the development of graphical password as an alternative. Graphical password which uses images as passwords, rather than alphanumeric characters is motivated particularly by the fact that it is generally easier for users to remember and recall images than words, and it is conceivable that graphical password would be able to provide better security than alphanumeric password.

In this thesis, a study of various schemes of graphical user authentication is made and a proposed graphical authentication scheme is implemented as an alternate to text-based authentication systems, various analysis are made and also several challenges in graphical authentication are discussed.

Contents

List of Figures

Chapter 1

Introduction

1.1 Introduction

Computer applications today uses user authentication as its fundamental security component. It provides the basis for access control and user accountability [1]. While there are various types of user authentication systems, alphanumerical username/passwords are the most common type of user authentication. They are versatile and easy to implement and use. Alphanumerical passwords are required to satisfy two contradictory requirements. They have to be easily remembered by a user, while they have to be hard to guess by impostor [2]. Users are known to choose easily guessable and/or short text passwords, which are an easy target of dictionary and brute-forced attacks [3]. Enforcing a strong password policy sometimes leads to an opposite effect, as a user may resort to write his or her difficult-to-remember passwords on sticky notes exposing them to direct theft.

Human factors are quite often considered as the weakest link in a computer system related with security. Patrick, et al. [4] pointed out three major areas where human-computer interaction is important: authentication, developing secure systems and security operations. Here we focus our attention to the authentication problem. The most common computer authentication method for a user is to

submit a username and a text password. The vulnerabilities of the alphanumeric method of authentication have been well known. One of the major problems is the difficulty in remembering passwords. Studies have also shown that many users tend to pick passwords that are easy to remember or a very short password [5]. Unfortunately, such passwords can easily be guessed or broken. According to a news article on Computerworld, a network password cracker was run by a security team at a large company and within 30 seconds, they were able to identify about 80% of the passwords [6]. In the contrary, passwords that are hard to break or guess are often very hard to remember unless one writes down in a piece of paper or somewhere. Studies showed that since user can only remember a limited amount of different passwords, they tend to use the same passwords for different accounts or write them down [7]. To counter the inherent problems with traditional username/password authentication, various alternative authentication methods, such as biometrics, have been used. In this thesis, however, we focus on graphical user authentication which is nothing but utilizing images as passwords. Graphical authentication schemes have been proposed as a possible alternative to replace the traditional username/password authentication schemes. It is motivated partially by the fact that humans are capable of remembering pictures or images better than texts; even psychological studies supports such assumption [8]. Pictures or images are generally much more easier to be remembered or recognized than that of textual objects. In addition to memorablity, if the number of possible pictures or images is significantly large, then the possible password space of a graphical password scheme may exceed that of text based schemes and thus might be able offer better resistance to dictionary attacks than text based schemes. Due to all these possibilities in mind, there is a growing interest in graphical user authentication. In addition to workstation and web log-in applications, graphical passwords have also been applied to mobile devices and ATM machines

1.2 Motivation

Today, authentication technology is the main measure to guarantee information security, and the most common and convenient authentication method is alphanumeric password. However, their inherent defects led to the search for an alternative way of authenticating users such as biometric authentication, which by the way is costly. On the other hand graphical authentication is a promising alternative to replace the traditional alphanumeric password way of authentication. The main motivation lies with the fact that the human brain is capable of remembering graphical or pictorial objects better than texts, even psychological studies support such assumptions. And also with the advancement of technology, we are now moving forward to using touch based devices such as mobile phones, tablets, and even touch screen monitors. So with this, the alphanumeric method is much more inconvenient in such touch based devices. So, the graphical method would allow the user to just touch the various regions in screen and get authenticated. With this in mind the graphical user authentication is likely to replace the traditional alphanumeric authentication method in the near future.

1.3 Structure of the Thesis

The rest of the thesis is organized as follows. Chapter 2 gives an overview of authentication methods and discuss various graphical authentication schemes and also various design implementation and security issues are discussed. Chapter 3 describes the proposed scheme for graphical user authentication and chapter 4 gives the detail of implementation of the proposed scheme. Chapter 5 presents the results and observations. Chapter 6 concludes the thesis and give direction for future research issues.

Chapter 2

Graphical Authentication

2.1 Overview of Authentication Methods

We can divide the authentication methods into three main areas:

- Token based authentication
- Biometric based authentication
- Knowledge based authentication

A token could be a small physical device that is owned by an authorized user of computer services to ease him in authentication. The token may be used in addition to a password or used in place of passwords to prove that the user is who they claim to be. The token acts like an electronic key to access something. Token based techniques, such as bank-cards, smart-cards and key-cards are widely used. Many of the token-based authentication systems also use knowledge based techniques so as to enhance the security. For example, ATM cards are constantly used together with a PIN number. So, token based authentication deals with what the user/person has.

Biometrics refers to the identification of human beings by their traits or characteristics. The authentication techniques based on biometric such as fingerprints, iris recognition, or face recognition, are not yet very widely adopted.

The major drawback of these approach is that such systems could be very expensive, and the process of identification can be slow and sometimes often unreliable. However, this type of authentication methods can provide the highest level of security. So, biometric based authentication deals with what the user/person is.

Knowledge based authentication methods can be considered as the most widely used authentication methods and include both text-based and picture-based authentication mechanism. In knowledge-based techniques, a user might be challenged with a set of images and the user passes the authentication by identifying and recognizing the images he or she selected during registration phase or a user might be asked to reproduce something that he or she created or selected earlier during the registration phase. So, knowledge based authentication deals with what the user/person knows.

As we can see, graphical authentication falls under knowledge based authentication and is discussed in more detail in the following sections.

2.2 Graphical Passwords

Graphical password can be defined as that, "Graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI)". For this reason, the authentication method in which graphical images or pictures are used as a password is sometimes called graphical user authentication (GUA). Many techniques have been designed in the field of graphical password since 1996. Existing graphical password schemes can be categorized into recall-based, recognition-based and cued-recall [9]. In the recall-based scheme, a user is asked to reproduce a pre-drawn outline drawing with the mouse or stylus on a grid. Recognition-based scheme requires the user to memorize a portfolio of images during password creation, and then recognize their images from among decoys during authentication. Cued-recall scheme, intends to

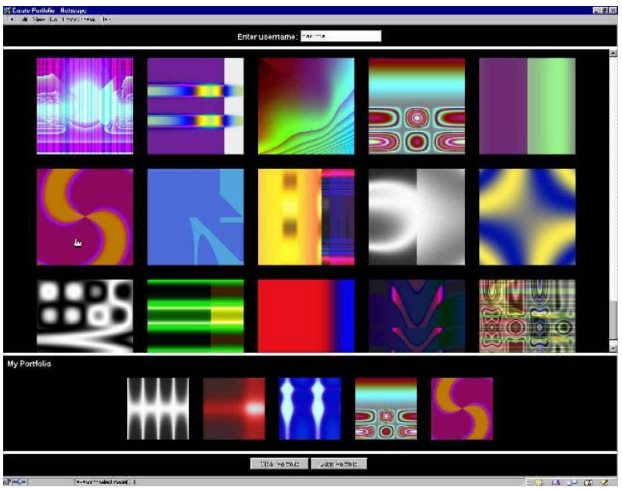

Figure 2.1: Graphical Authentication scheme by Dhamija and Perrig

reduce the memory load on users, generally provides a background image and the user must remember and target specific locations on the image. Also, the graphical user authentication system implemented in this thesis is based on the cued-recall scheme.

2.2.1 Recognition Based Techniques

Dhamija and Perrig [7] proposed a graphical authentication scheme based on the Hash Visualization technique [8]. In their authentication system, user selects a certain number of images from a set of program generated random pictures (Figure 2.1). For a user to be authenticated, he or she would have to identify the pre-selected images. One weakness of their system is that the server needs to store the seeds of the selected images of each user in plain text. Also, it is a bit time consuming and tedious for the users to select images from the database.

Akula and Devisettys algorithm [10] is similar to the technique proposed by Dhamija and Perrig [7]. The main difference is that they make the authentication more secure and require less memory. They did this by using hash function SHA-1, which produces a 20 byte output. The authors also suggested that this could be deployed on the Internet, cell phones and PDA's.

Weinshall and Kirkpatrick [11] proposed and study several authentication schemes. They conducted a number of user studies. The various studies includes picture recognition, object recognition, and pseudo word recognition. In the picture recognition study, out of a database of 20,000 images, a large set of images are selected (100-200 images). Then the user is trained to recognize those set of images. After one to three months, users in their study were able to recognize over 90% of the images in the training set. This study showed that pictures are the most effective among the three schemes tested. Pseudo codes can also be used, but require proper setting and training.

Sobrado and Birget [12] developed a graphical authentication technique that is considered to be shouldersurfing resistant. In the first scheme, the system will display a number of pass-objects (pre-selected by user) among many other objects. To be authenticated, a user needs to recognize pass-objects and click inside the convex hull formed by all the pass-objects (Figure 2.2). In order to make the password hard to guess, Sobrado and Birget suggested using 1000 objects, which makes the display very crowded and the objects almost indistinguishable, but using fewer objects may lead to a smaller password space, since the resulting convex hull can be large. In their second algorithm, a user moves a frame (and the objects within it) until the pass object on the frame lines up with the other two passobjects. The authors also suggest repeating the process a few more times to minimize the likelihood of logging in by randomly clicking or rotating. The major disadvantage of their scheme is that, the authentication phase or login phase could be very slow.

Man, et al. [13] proposed another shoulder-surfing resistant algorithm. In their method, a user selects a number pass-objects which are nothing but thumbnails of images. Each pass-object has several variants and each variant is assigned a unique code. During authentication, the user is challenged with several scenes. Each scene contains several pass-objects (each in the form of a randomly chosen

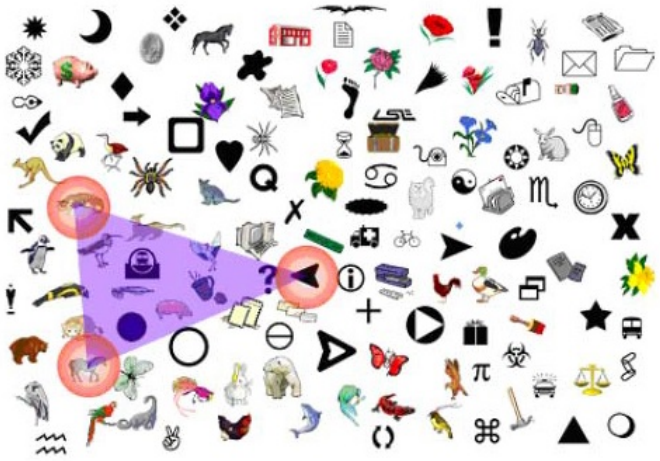

Figure 2.2: Graphical Authentication scheme by Sobrado and Birget

variant) and many decoy-objects. The user has to type in a string with the unique codes corresponding to the pass-object variants present in the scene as well as a code indicating the relative location of the passobjects in reference to a pair of eyes. The argument is that it is very hard to crack this kind of password even if the whole authentication process is recorded on video because where is no mouse click to give away the pass-object information. However, this method still requires users to memorize the alphanumeric code for each pass-object variant. Hong, et al. [14] later extended this approach to allow the user to assign their own codes to pass-object variants. Figure 2.3 shows the log-in screen of this graphical password scheme. However, this method still forces the user to memorize many text strings and therefore suffer from the many drawbacks of text-based passwords.

A technique called "Passface" is developed by Real User Corporation [15]. The basic idea is as follows. The user have to choose four images of human faces from a face database. These selected faces are stored as their password. In the authentication stage, the user is presented with a grid consisting of nine faces, consisting of one face previously chosen by the user and eight decoy faces (Figure 2.4). The user recognizes and clicks anywhere on the known face. This procedure is repeated for several rounds. The user is authenticated if he/she correctly identifies

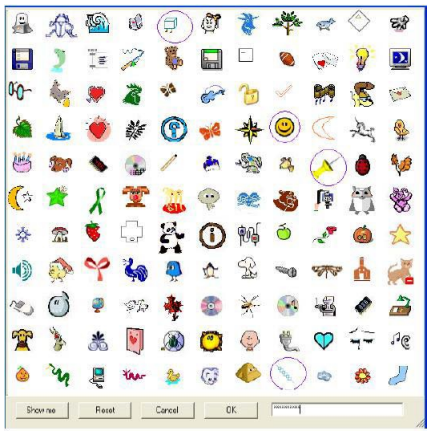

Figure 2.3: Graphical Authentication scheme by Hong, et al

the four faces. The technique is based on the assumption that people can recall human faces easier than other pictures. User studies by Valentine [16, 17] have shown that Passfaces are very memorable over long intervals. Comparative studies conducted by Brostoff and Sasse [18] showed that Passfaces had only a third of the login failure rate of text-based passwords, despite having about a third the frequency of use. Their study also showed that the Passface-based login process took longer than text passwords and therefore was used less frequently by users. However the effectiveness of this method is still uncertain. Davis, et al. [19] studied the graphical passwords created using the Passface technique and found obvious patterns among these passwords. For example, most users tend to choose faces of people from the same race. This makes the Passface password somewhat predictable. This problem may be alleviated by arbitrarily assigning faces to users, but doing so would make it hard for people to remember the password.

Jansen [20] proposed a graphical password mechanism for mobile devices. During the enrollment stage, a user selects a theme (e.g. sea, cat, etc.) which consists of thumbnail photos and then registers a sequence of images as a password (Figure 2.5). During the authentication, the user must enter the registered images in the correct sequence. One drawback of this technique is that since the number of thumbnail images is limited to 30, the password space is small. Each thumbnail image is

Figure 2.4: Passface Graphical Authentication scheme

Figure 2.5: Graphical Authentication scheme by Jansen et al.

assigned a numerical value, and the sequence of selection will generate a numerical password. The result showed that the image sequence length was generally shorter than the textural password length. To address this problem, two pictures can be combined to compose a new alphabet element, thus expanding the image alphabet size.

Takada and Koike discussed a similar graphical password technique for mobile devices. This technique allows users to use their favorite image for authentication [21]. The users first register their favorite images (pass-images) with the server.

During authentication, a user has to go through several rounds of verification. At each round, the user either selects a pass-image among several decoy-images or chooses nothing if no pass-image is present. The program would authorize a user only if all verifications are successful. Allowing users to register their own images makes it easier for user to remember their pass-images. A notification mechanism is also implemented to notify users when new images are registered in order to prevent unauthorized image registration. This method does not necessarily make it a more secure authentication method than text-based passwords. As shown in the studies by Davis [19], user's choices of picture passwords are often predictable. Allowing users to use their own pictures would make the password even more predictable, especially if the attacker is familiar with the user.

2.2.2 Recall Based Techniques

In this section we discuss two types of picture password techniques: reproducing a drawing and repeating a selection.

- **Reproduce a Drawing**

  Jermyn, et al. [22] proposed a technique, called "Draw-a-secret (DAS)", which allows the user to draw their unique password (Figure 2.6). A user is asked to draw a simple picture on a 2D grid. The coordinates of the grids occupied by the picture are stored in the order of the drawing. During authentication, the user is asked to re-draw the picture. If the drawing touches the same grids in the same sequence, then the user is authenticated. Jermyn, et al. suggested that given reasonable-length passwords in a 5 X 5 grid, the full password space of DAS is larger than that of the full text password space.

  Syukri, et al. [23] proposes a system where authentication is conducted by having the user drawing their signature using a mouse (Figure 2.7). Their technique included two stages, registration and verification. During the registration stage: the user will first be asked to draw their signature with

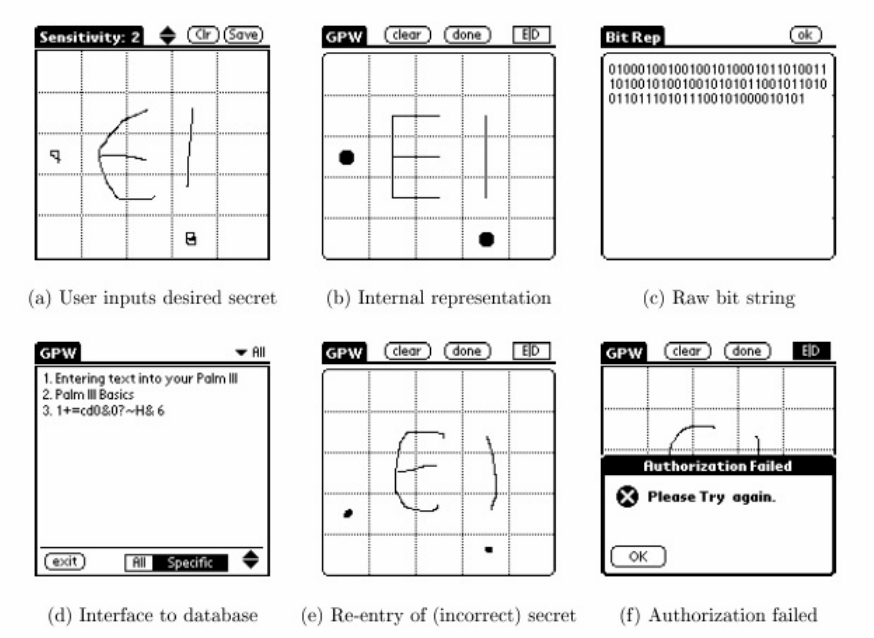

Figure 2.6: DAS authentication technique

a mouse, and then the system will extract the signature area and either enlarge or scale-down the signature, and rotates if needed, (also known as normalizing). The information will later be saved into the database. The verification stage first takes the user input, and does the normalization again, and then extracts the parameters of the signature. After that, the system conducts verification using geometric average means and a dynamic update of the database. According to the paper the rate of successful verification was satisfying. The biggest advantage of this approach is that there is no need to memorize ones signature and signatures are hard to fake. However, not everybody is familiar with using a mouse as a writing device; the signature can therefore be hard to draw. One possible solution to this problem would be to use a pen-like input device, but such devices are not widely used, and adding new hardware to the current system can be expensive. We believe such a technique is more useful for small devices such as a PDA, which may already have a stylus.

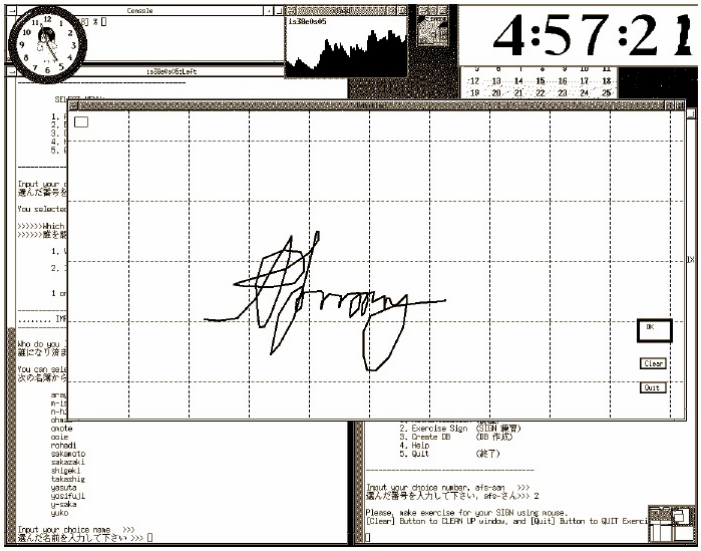

Figure 2.7: Signature drawn by mouse

- **Repeat a sequence of actions**

  Blonder [24] designed a graphical password scheme in which a password is created by having the user click on several locations on an image. During authentication, the user must click on the approximate areas of those locations. The image can assist users to recall their passwords and therefore this method is considered more convenient than unassisted recall (as with a text-based password). Passlogix has developed a graphical password system based on this idea. In their implementation (Figure 2.8), users must click on various items in the image in the correct sequence in order to be authenticated. Invisible boundaries are defined for each item in order to detect whether an item is clicked by mouse. It was reported that Microsoft had also developed a similar graphical password technique where users are required to click on pre-selected areas of an image in a designated sequence [25]. But details of this technique have not been available.

  The "PassPoint" system by Wiedenbeck, et al. [26] extended Blonder's idea by eliminating the predefined boundaries and allowing arbitrary images to be

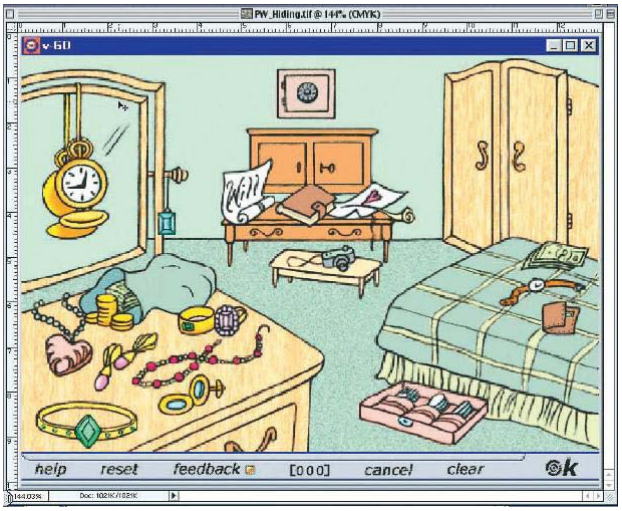

Figure 2.8: A recall-based technique developed by Passlogix

used. As a result, a user can click on any place on an image (as opposed to some pre-defined areas) to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, the user must click within the tolerance of their chosen pixels and also in the correct sequence (Figure 2.9). Because any picture can be used and because a picture may contain hundreds to thousands of memorable points, the possible password space is quite large. However, their studies showed that graphical password users had more difficulties learning the password, and took more time to input their passwords than the alphanumerical users.

Passlogix has also developed several graphical password techniques based on repeating a sequence of actions. For example, its v-Go includes a graphical password scheme where users can mix up a virtual cocktail and use the combination of ingredients as a password. Other password options include picking a hand at cards or putting together a "meal" in the virtual kitchen. However, this technique only provides a limited password space and there is no easy way to prevent people from picking poor passwords.

A Novel Cued-recall Graphical Password Scheme by Xiyang Liu et.al [27]

Figure 2.9: An image used in the Passpoint Sytem

proposed a scheme CBFG(Click Buttons according to Figures in Grids) inherits the basic principle of Passpoints during the password creation, and introduces the ideology of image identification. CBFG can be considered as an improvement of Passpoints, as it keeps the advantage of large password space of Passpoints and achieves some better performances. It adopts multiple background images for the first time. Operating on password regions indirectly at authentication stage, dispensing with recall of passwords order and hiding the key information of user input sequence bring some improvements to CBFG both in usability and security: users tend to set more complex passwords, users memory burden is reduced and the scheme can resist shoulder surfing attack.

2.3 Security Analysis of Graphical Authentication

Enough research is yet to be undertaken to study the difficulty of cracking graphical passwords. As graphical passwords are still not widely used in real world

applications, there is no report on real cases of breaking graphical passwords. Here we briefly exam some of the possible techniques for breaking graphical passwords and try to do a comparison with text-based passwords.

- **Brute force search**

  The main defense measure against brute force search is to have a sufficiently large password space. Text-based passwords have a password space of 94^N, where N is the length of the password, 94 is the number of printable characters (shift and non-shift keys excluding SPACE) on a standard keyboard. Some graphical password techniques have been shown to provide a password space similar to or larger than that of text-based passwords [28]. Recognition based graphical passwords tend to have smaller password spaces than the recall based methods. It is more difficult to carry out a brute force attack against graphical passwords than text-based passwords. The attack programs need to automatically generate accurate mouse motion to imitate human input, which is particularly difficult for recall based graphical passwords. Overall, in terms of brute force attacks, it is believed that a graphical password has less vulnerability than a text-based password.

- **Dictionary attacks**

  It is impractical to carry out dictionary attacks against graphical passwords as recognition based graphical passwords involve mouse input instead of keyboard input. For some recall based graphical passwords [22], it is possible to use a dictionary attack but an automated dictionary attack will be much more complex than a text based dictionary attack. More research is needed in this area. However, it is evident that graphical passwords has less vulnerability to dictionary attacks than text-based passwords.

- **Spyware**

  Except for few cases, key listening or key logging spyware cannot be used to break graphical passwords. It is not clear whether "mouse tracking" spyware

will be an effective tool against graphical passwords. However, motion of the mouse alone is not enough to break graphical passwords. Such information has to be correlated with application information, such as window location, its position and size, as well as desktop resolution and size also matters.

- **Shoulder surfing**

  Like text based passwords, most of the graphical authentication methods are vulnerable to shoulder surfing. Uptil now, only a few recognition-based methods claim to resist shoulder-surfing. None of the recall-based based methods are considered should-surfing resistant.

- **Social engineering**

  It is less convenient for a user to give away graphical passwords to another person as compared to text based passwords. For instance, to tell a graphical password to others over the phone would be very difficult. Even if an attacker is to set up a phishing website so as to obtain graphical passwords from targetted users, it would be more time consuming to set up such sites. Overall, it is more difficult to break graphical passwords using the traditional attack methods like brute force search, dictionary attack, and spy-ware. As graphical passwords are still not widely deployed, an in-depth research and studies that investigates possible attack methods are still needed.

2.4 Design and Implementation Issues of Graphical Passwords

- **Security**

  We have briefly examined the security issues with graphical passwords already in the above section.

- **Usability**

  One of the major argument for graphical authentication is that images are much more easier to remember than text strings. Some research papers presented preliminary user studies to support this. However, current user studies involves only a small number of users and are still very limited. But it is still difficult to be convinced that graphical passwords are easier to remember than text based passwords as we do not have enough evidence.

  A major complaint among the users of graphical authentication procedure is that the registration process and log-in process take too much time, especially in recognition-based approaches. For instance, in the registration phase, a user has to pick few images from a larger number of image sets. Then in the authentication phase, a user has to identify a few pass-images by scanning through all the images displayed. Users may find this process long and tedious. Due to this users often find graphical passwords less convenient than text based passwords. And also most users are not familiar with the graphical passwords.

- **Reliability**

  The major design issue for recall-based methods is the reliability and accuracy of user input recognition. The error tolerances in graphical authentication schemes have to be set carefully if the tolerances are overly high then it may lead to many false positives. And if the tolerances are overly low, then again it may lead to many false negatives. In addition, if the program is more error tolerant, then it will be more vulnerable to attacks.

- **Communication and Storage**

  Graphical authentication schemes require much more space for storage than text based passwords. Huge numbers of images may have to be maintained in a centralized storage database. The delay in loading or transfer of images is also a

concern for graphical authentication schemes. Especially for recognition-based techniques in which a large number of images may need to be displayed for each round of verification in the authentication process.

Chapter 3

Proposed Scheme

The graphical authentication scheme that is proposed in this thesis is based on the cued recall authentication scheme, in which the user would have to remember a sequence of clicked points on an image to be authenticated. The scheme is made simple so as to avoid much stress to the user while registration and logging in to the system in order to increase usability.

Registration Phase

In the registration phase, user enters a username that has not already been taken by another user and then chooses his password by clicking several interest points on the displayed image. The coordinates of the clicked points are collected and stored in the database along with the entered username.

Authentication Phase

In the authentication phase user enters his username and then click on interest points on the displayed image in the same sequence that he had done during registration phase. The entered username and coordinates of the clicked points are matched against the one stored in the database. If a match is found, user is successfully authenticated, otherwise the user will not be allowed to access the system.

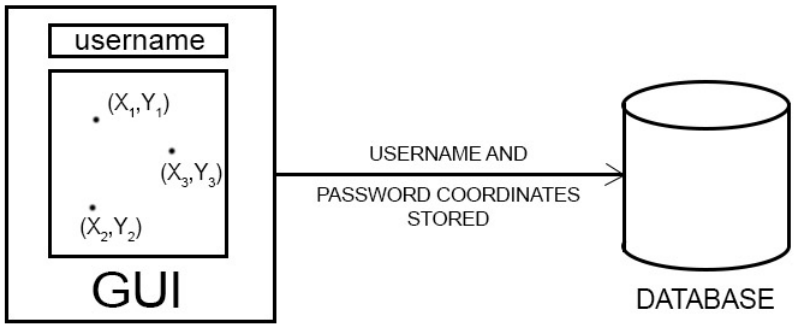

Figure 3.1: Registration phase of Proposed Scheme

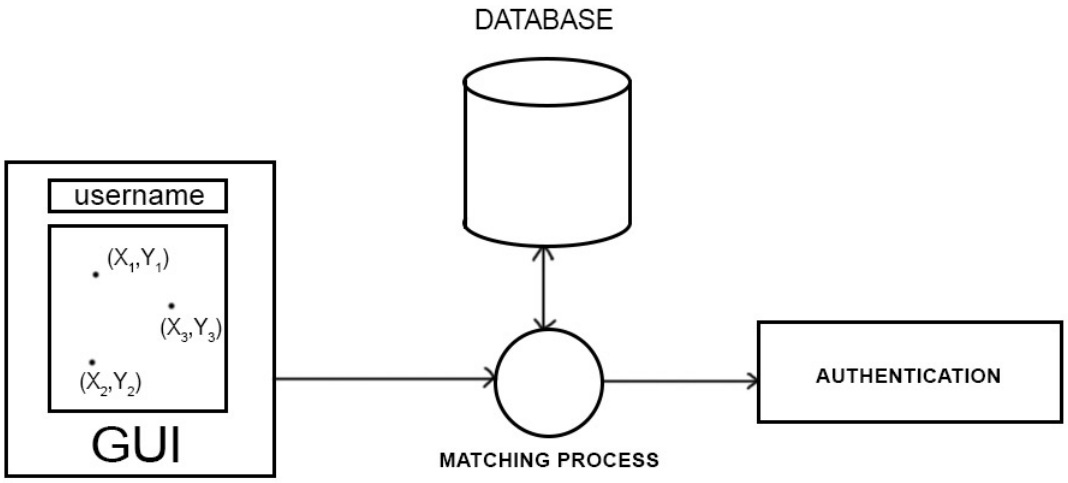

Figure 3.2: Authentication phase of Proposed Scheme

The graphical authentication scheme proposed here uses two fixed images of 600x400px each during registration and authentication. In this scheme the user have to click six points, three on each image as his or her password. The first image is displayed first and as soon as the user selected or clicked three times on the first image, the second image appears, the user can then select or click another three points.

Unlike most graphical authentication systems implemented, in our proposed scheme we do not divide the image into grids. Rather we are giving the users freedom to click on any points they like. Now, since we do not divide the image into grids, it is unlikely that a user would click exactly at the same pixel point on the image, we have to make some threshold or tolerance upto which a deviation from the original point is considered as the correct points. In our proposed scheme we have chosen a 15px radius around the original point to be considered as the threshold radius. This means that a user have to click within a 30x30px area. In other literature where they have used grids we see that they have used a 40x40px cell for the grid. Although a 40x40px cell is quite optimal, a 30x30px is much more secure and pose no harm as the user tends to be more careful.

Chapter 4

Implementation

We implemented our proposed scheme on a web-based environment. We have used the following technologies for the implementation:

- PHP as the core programming tool
- MySQL for database storage
- Apache server
- Javascripts and Ajax
- CSS

WAMP server was installed in a Windows 8 machine and Google Chrome browser was used to run the webpages.

4.1 Database Setup

As mentioned earlier we have used MySQL database for storing the username and passwords (coordinates) of the users. We created just one table named 'users' with 14 columns namely id, username, x0, y0, x1, y1, x2, y2, x3, y3, x4, y4, x5, y5. These stores the username and the various (x,y) coordinates in seperate columns. Figure 4.1 shows a screenshot of our database table as seen through *phpMyAdmin()*.

	id	username	x0	y0	x1	y1	x2	y2	x3	y3	x4	y4	x5	y5
Edit Copy Delete	1	maxeer	317	218	317	218	317	218	317	218	317	218	317	218
Edit Copy Delete	2	user2	318	205	618	149	476	419	267	77	140	389	621	220
Edit Copy Delete	11	<?php hello echo "\" echo "hello">	97	102	201	104	237	247	434	210	423	113	139	345
Edit Copy Delete	22	this thatz	289	58	266	292	512	251	506	105	194	127	315	265
Edit Copy Delete	31	bollot	506	62	213	93	249	314	434	274	279	59	154	229
Edit Copy Delete	32	Hello GÃ¼nter	243	78	445	73	337	230	258	76	189	212	515	265
Edit Copy Delete	33	newuser""	450	53	249	150	412	264	471	159	179	154	402	275
Edit Copy Delete	34	hellomp	53	20	262	161	409	99	373	191	197	206	485	216
Edit Copy Delete	35	joiplolo	56	43	333	102	252	274	40	308	482	104	519	269
Edit Copy Delete	36	testuser	149	80	488	110	317	294	465	317	339	112	174	263
Edit Copy Delete	37	testuser2	150	80	235	162	339	385	326	5	316	219	341	262
Edit Copy Delete	38	lalop	288	135	494	251	228	284	500	85	207	79	31	62
Edit Copy Delete	39	hellopop	220	63	74	191	461	254	251	156	182	299	473	291
Edit Copy Delete	40	any name	157	84	241	161	331	377	323	14	319	219	350	272
Edit Copy Delete	41	user1	155	80	245	165	339	381	101	109	368	217	511	311

Figure 4.1: Database table structure

4.2 Layout Design

The home page consists of two buttons: Login and Register button. The login button redirects the user to login page and the Register button redirects to registration page. The screenshots of various pages are shown in the next section.

The Register page consists of a text field where user can enter a username and when a new user enters a username in the field the database is checked for availability of that particular username. If a chosen username already exists in the database then an indication appears on the right side of the field whether or not the entered username is available. Now, after entering a username, the user clicks on any points on the image, after 3 clicks, the image is replaced by a second image, then the user clicks another 3 points. If the username is not left blank and an available username is used, the user data is stored into the database. If registration is successful, then a success message is shown on a new page and if registration is unsuccessful a failure message is shown on a new page.

The Login page is similar to the register page except that the username is not checked for availability. Instead when the user clicks all the points in the image,

it checks whether the clicked points are within the tolerance region of the original points stored in the database. If all the points are correct and in the same sequence then the user is logged in successfully and a success message is shown in a new page, otherwise a failed login message page is shown.

4.3 Screenshots

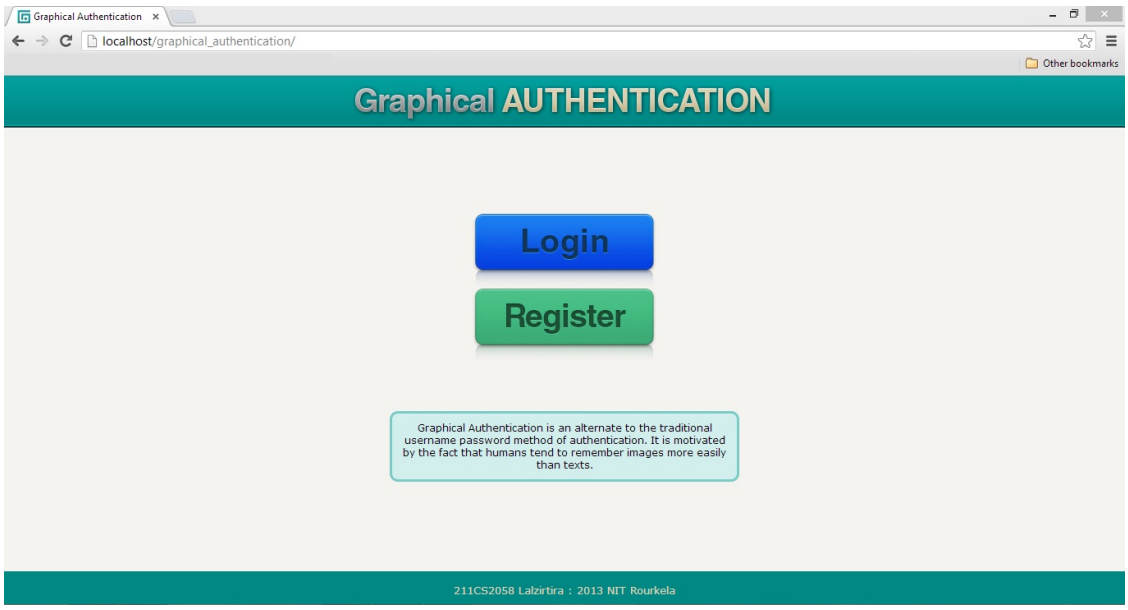

Figure 4.2: Home page

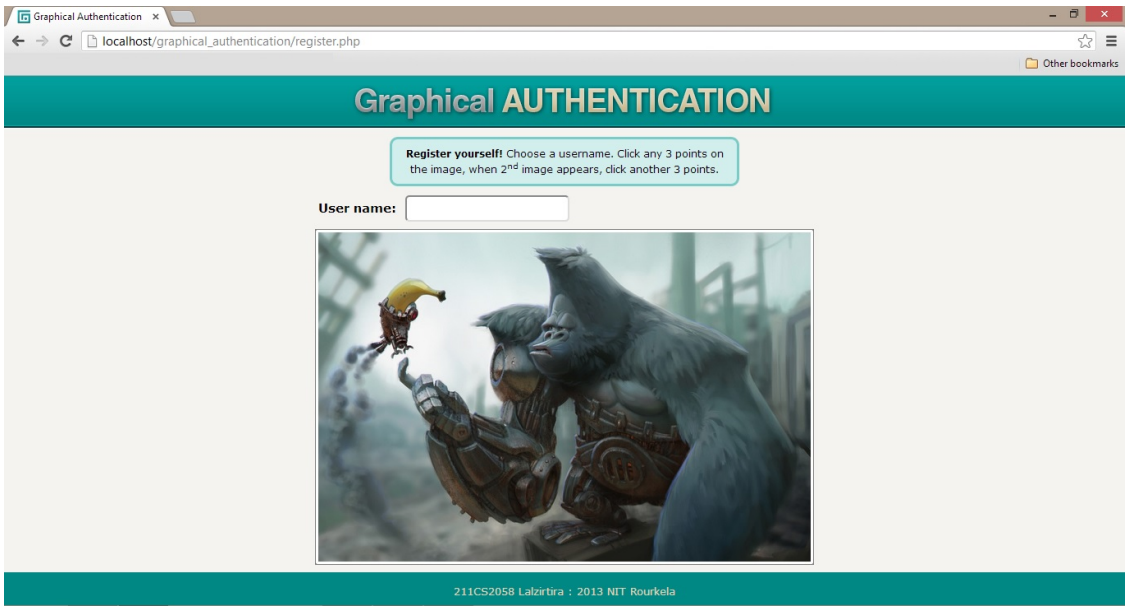

Figure 4.3: Register page

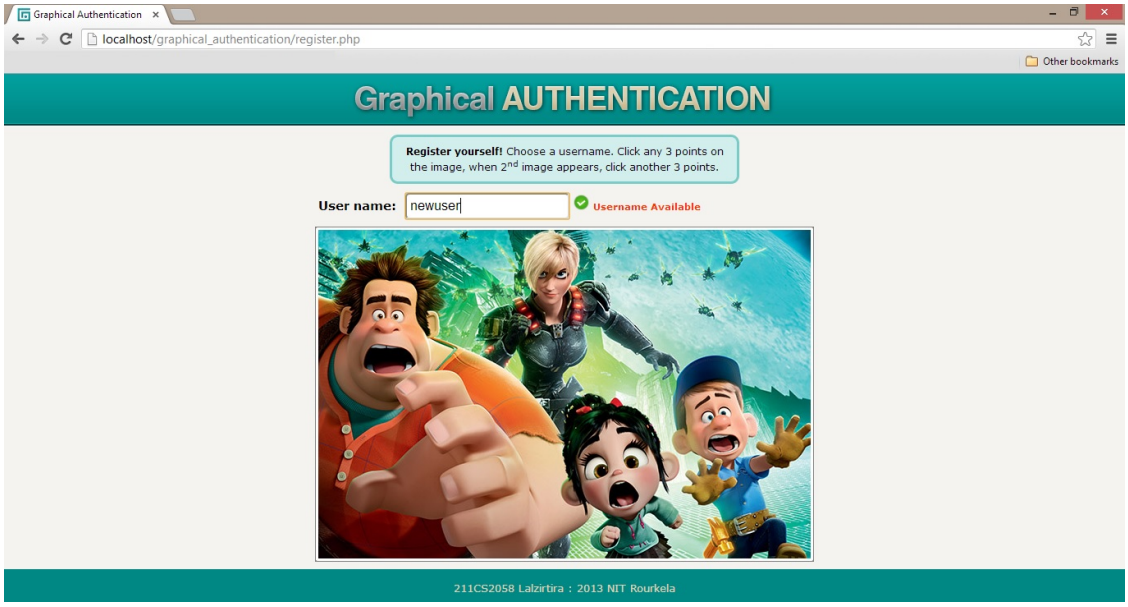

Figure 4.4: Register page showing a second image and username availibility indicator

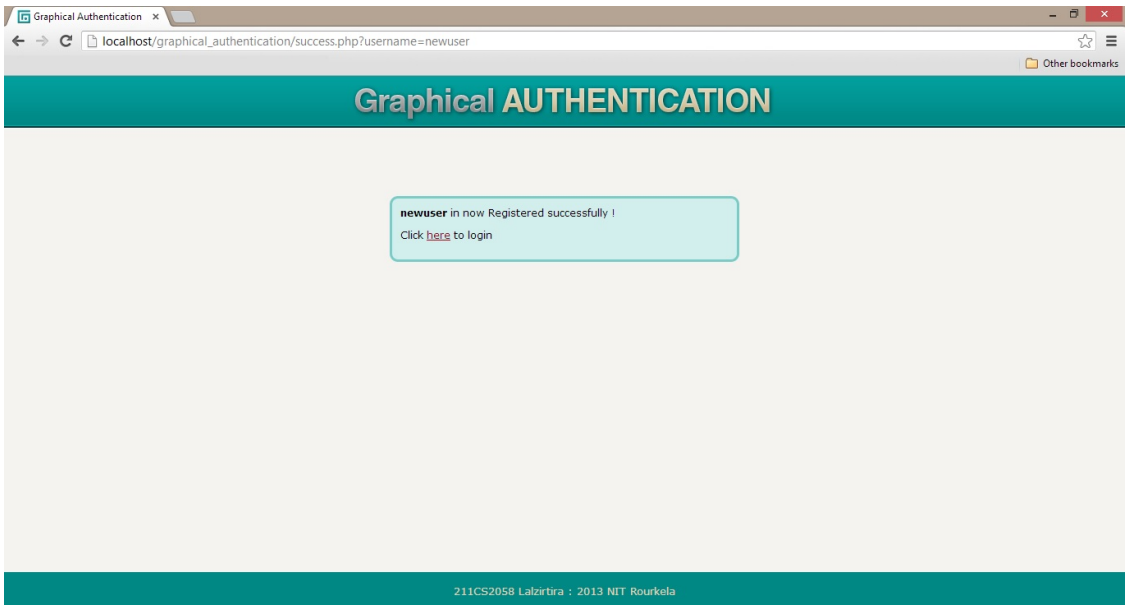

Figure 4.5: Registration success message page

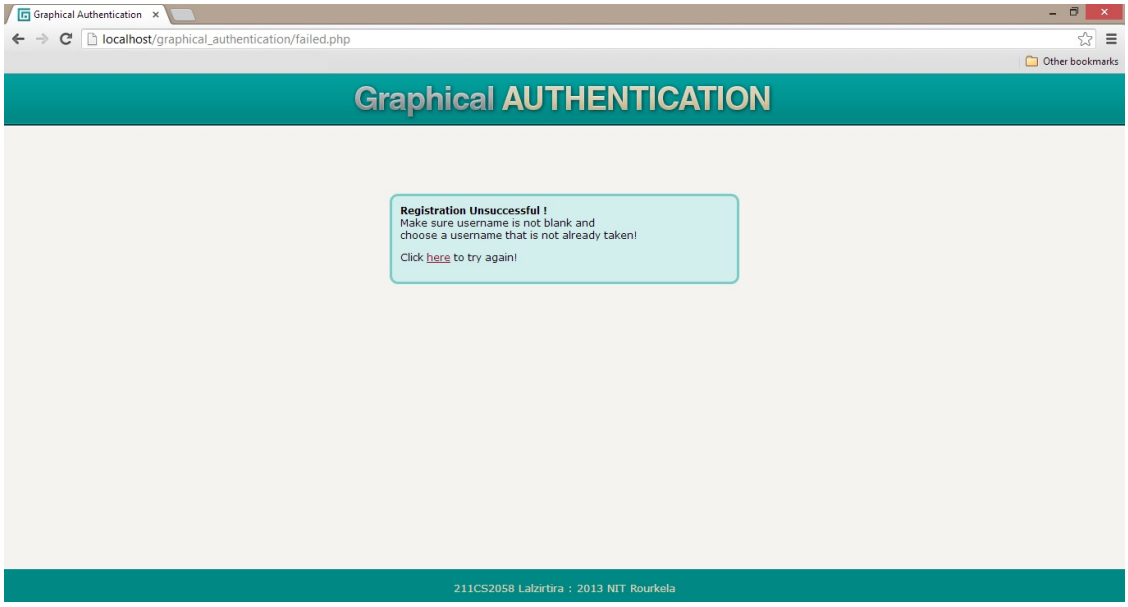

Figure 4.6: Registration failure message page

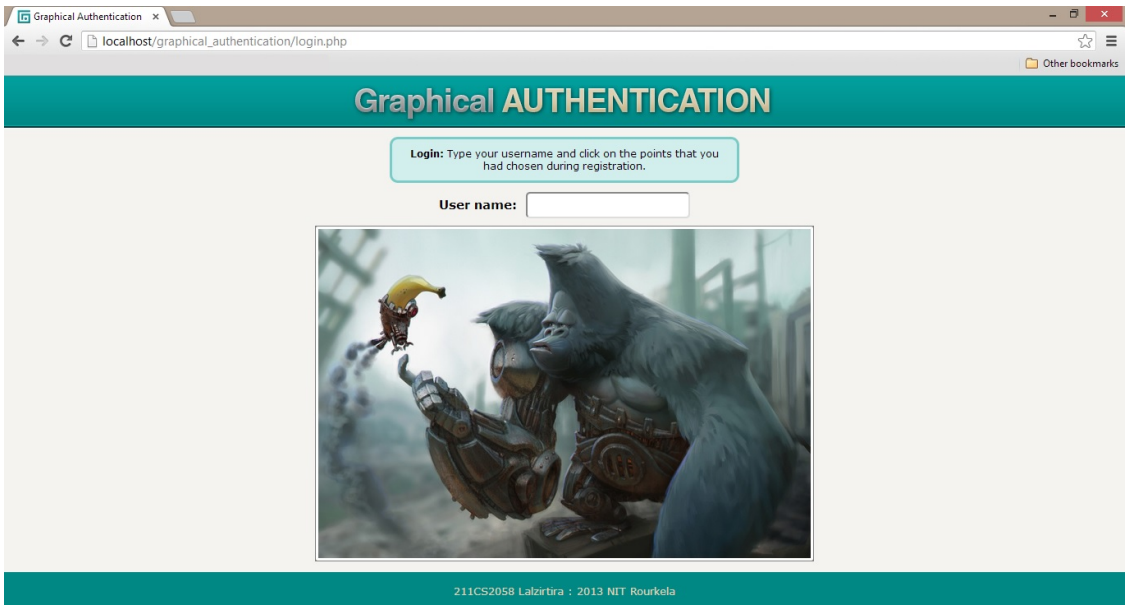

Figure 4.7: Login page

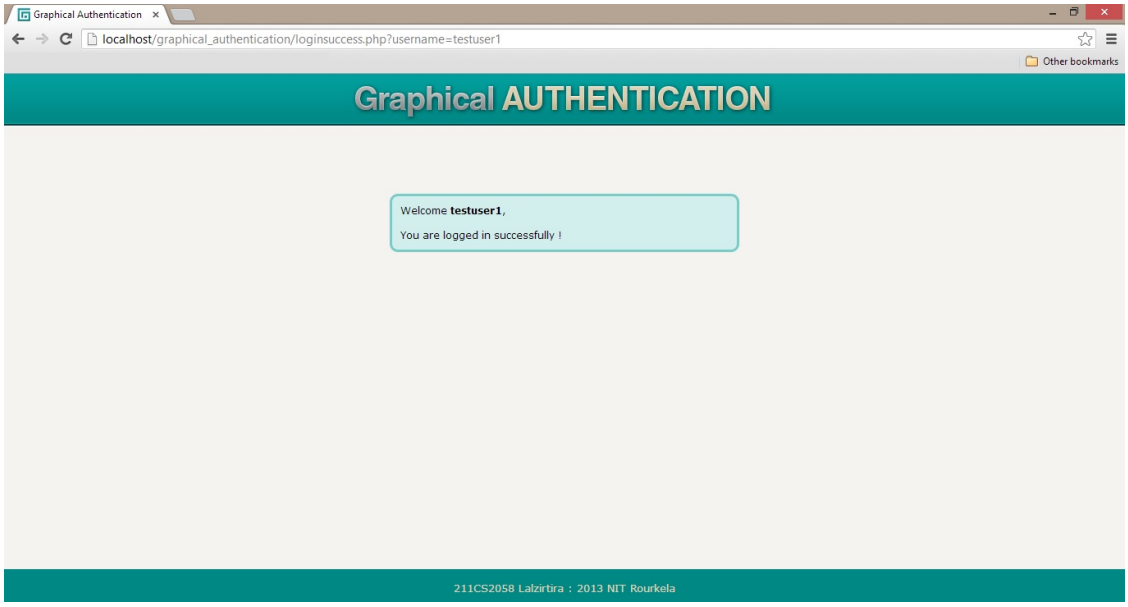

Figure 4.8: Login Success message page

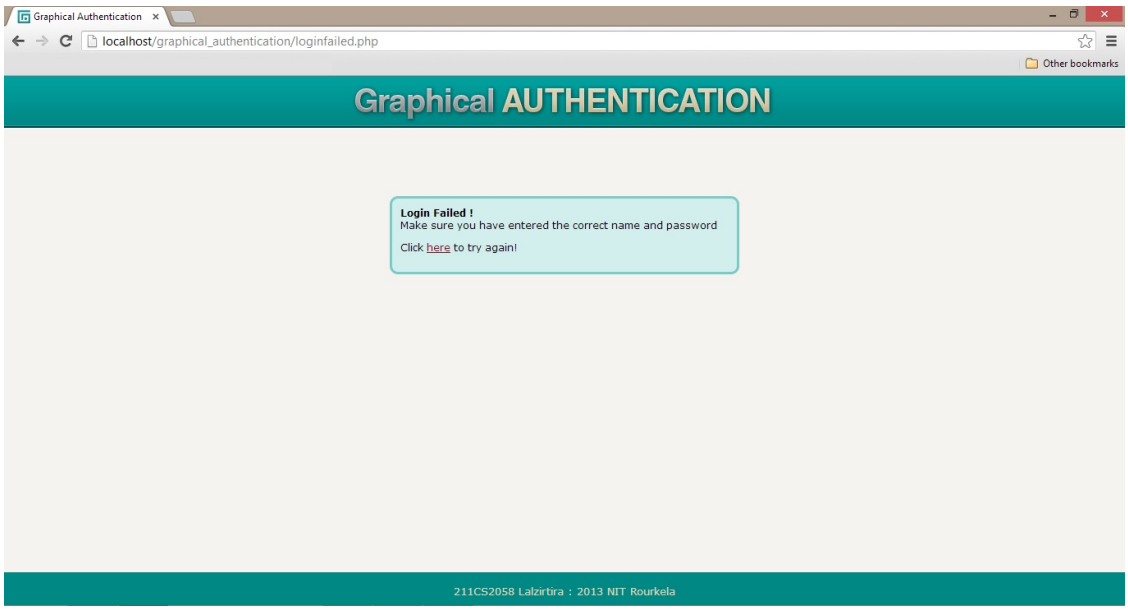

Figure 4.9: Login Failed message page

Chapter 5

Results and Discussions

5.1 Key Space Analysis

A simple key space analysis of the clickable ranges on our graphical authentication system prototype is compared to that of an alphanumeric authentication system. Each click on the graphical image is equivalent to a typed character in a normal password. Assuming the 94 available keys (shift and non-shift characters excluding SPACE on a standard keyboard), an alphanumeric password whose length is 'n' would have a key space of 94^n. And since we use a 600x400px image and with a tolerance bound of 30px, we can consider our image as a 20x13 unique grids, so each click of the image has around 260 possible values, so a sequence of n clicks has a key space of 260^n. Figure 5.1 shows the increase in size of key space based on alphanumeric methods versus image clicks (graphical passwords) for increasingly large passwords.

Brute Force Search

It is clear from Figure 5.1 that our graphical authentication scheme has larger password space than that of alphanumeric password. We can say that our scheme is less vulnerable to brute force attack than a text based password.

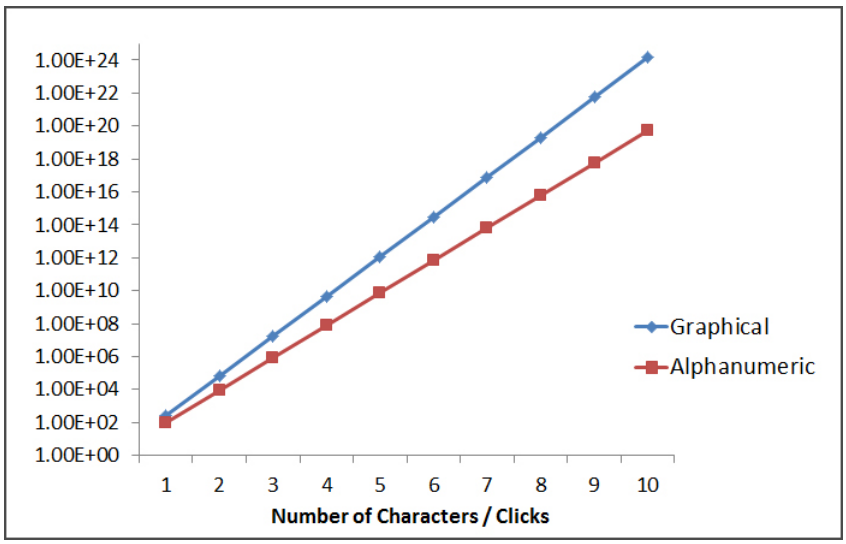

Figure 5.1: Key space for alphanumeric and graphical passwords

Dictionary Attacks

Since our graphical authentication scheme involves mouse input, it is quite impractical to carry out dictionary attacks. Even if it is possible somehow, it will be more difficult to carry our dictionary attacks on graphical password than that of text-based password.

5.2 Usability Analysis

Usability analysis of our graphical authentication scheme was carried out by experimenting with 10 different users who provided feedback on its usability and memorability. On a survey on the user's rating of the authentication scheme on a scale of 1 to 5 (1 being difficult and 5 being easy), we obtain an average rating of 3.4. In terms of memorability, 70% of the users feel that it is easier to remember than alphanumeric, and the rest feel that it is quite equivalent. In terms of registration and login time duration, our graphical authentication scheme obviously takes much more time to complete. Also the success rate of user login in their first attempt is 100%, which is quite impressive.

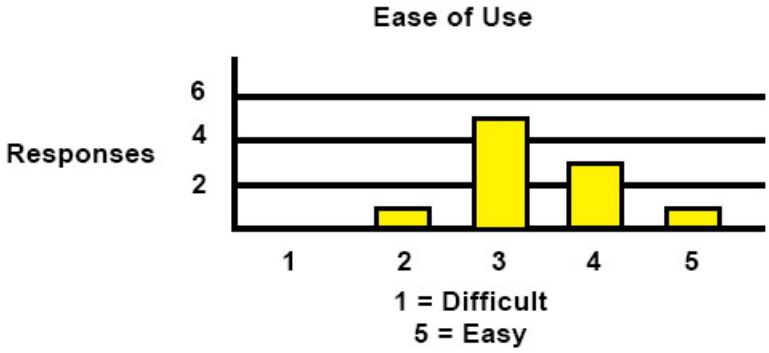

Figure 5.2: User survey on ease of use

5.3 Limitations

The limitations in our graphical authentication schemes may be noted as follows:

Our scheme is not safe from shoulder surfing problem. Based on the literature survey of various graphical scheme, it is evident that a system that claims to have no shoulder surfing problem have more complications in their authentication method and that the usability or ease of use is drastically decreased. So in order to maintain the ease of use we have not look into the shoulder surfing prevention mechanisms, in fact it is advisable that the user should be careful for such kind of attacks.

Our database is not encrypted in our scheme. As our authentication system that we implemented is just a kind of a prototype, all the aspects of security are not taken into considerations.

Our authentication scheme do not ask the user to re-enter their password at the time of registration, this could cause a user who is not paying much attention to easily forget his password right after he is being registered.

5.4 Other Observations

Our observation shows that user tends to choose and click on predictable areas or spots such as in our case the eyes, nose, etc, of the picture. This creates 'hot-spots' which is a well-known weakness in the underlying technique. Users also tend not to choose blank areas such as clear sky regions etc., this makes the password space to become smaller.

Our observation also reveals that the users being used to text-based authentication are finding it a bit hard to work on such graphical authentication schemes. This is evident from the fact that users tend to spent a lot more time authenticating themselves as compared to the time taken in text-based authentication methods.

Chapter 6

Conclusion

The thesis presented a graphical user authentication scheme as an alternative to replace text based authentication system. The proposed system is based on the cued-recall authentication scheme in which a user is presented with a background image and he has to click on several points in a sequence. A prototype of the proposed model was implemented on a web platform using PHP.

Results showed that graphical authentication has a high usability and that it is likely to replace text-based authentication methods in the near future. And even as of today, we can see graphical passwords being used in Windows8 OS as an alternate to text password, and also in touch based handheld devices like android smartphones, we see pattern locking mechanisms which is nothing but graphical authentication.

So with the advancement in technology mainly in touch based technology, graphical authentication plays a very promising role for various authentication in such devices or gadgets.

Future Work

As of now graphical authentication still needs a lot of research in order to be deployed in a large scale environment, and also the problem of shoulder-surfing needs to be looked deeper. And also for a web-based graphical authentication scheme in particular much research is needed so as to be able to work fluently in all various sizes of web devices.

Also, as there is yet no wide deployment of graphical password systems, the vulnerabilities are yet to be exploited. Much more user studies and research are necessary for graphical user authentication methods to achieve higher levels of usefulness and maturity.

Bibliography

[1] William Stallings and Lawrie Brown. *"Computer Security: Principle and Practices."* Pearson Education, 2008.

[2] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. *"Passpoints: Design and Longitudinal Evaluation of a Graphical Password System."* International Journal of Human-Computer Studies, 63:102127, July 2005.

[3] Daniel V. Klein. *"Foiling the Cracker: A Survey of, and Improvements to, Password Security."* In Proceedings of the 2nd USENIX UNIX Security Workshop, 1990.

[4] A. S. Patrick, A. C. Long, and S. Flinn, *"HCI and Security Systems,"* presented at CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA., 2003.

[5] A. Adams and M. A. Sasse, *"Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures,"* Communications of the ACM, vol. 42, pp. 41-46, 1999.

[6] K. Gilhooly, *"Biometrics: Getting Back to Business,"* in Computerworld, May 09, 2005.

[7] R. Dhamija and A. Perrig, *"Deja Vu: A User Study Using Images for Authentication,"* in Proceedings of 9th USENIX Security Symposium, 2000.

[8] R. N. Shepard, *"Recognition memory for words, sentences, and pictures,"* Journal of Verbal Learning and Verbal Behavior, vol. 6, pp. 156-163, 1967.

[9] X. Suo, Y. Zhu and G. Owen, *"Graphical Passwords: A Survey,"* In Proc. ACSAC 2005.

[10] S. Akula and V. Devisetty, *"Image Based Registration and Authentication System,"* in Proceedings of Midwest Instruction and Computing Symposium, 2004.

[11] D. Weinshall and S. Kirkpatrick, *"Passwords Youll Never Forget, but Cant Recall,"* in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402.

[12] L. Sobrado and J.-C. Birget, *"Graphical passwords,"* The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.

[13] S. Man, D. Hong, and M. Mathews, *"A shouldersurfing resistant graphical password scheme,"* in Proceedings of International conference on security and management. Las Vegas, NV, 2003.

[14] D. Hong, S. Man, B. Hawes, and M. Mathews, *"A password scheme strongly resistant to spyware,"* in Proceedings of International conference on security and management. Las Vergas, NV, 2004.

[15] RealUser, *"www.realuser.com."*

[16] T. Valentine, *"An evaluation of the Passface personal authentication system,"* Technical Report, Goldsmiths College, University of London 1998.

[17] T. Valentine, *"Memory for Passfaces after a Long Delay,"* Technical Report, Goldsmiths College, University of London 1999.

[18] S. Brostoff and M. A. Sasse, *"Are Passfaces more usable than passwords: a field trial investigation,"* in People and Computers XIV - Usability or Else: Proceedings of HCI. Sunderland, UK: Springer-Verlag, 2000.

[19] D. Davis, F. Monrose, and M. K. Reiter, *"On user choice in graphical password schemes,"* in Proceedings of the 13th Usenix Security Symposium. San Diego, CA, 2004.

[20] W. Jansen, *"Authenticating Mobile Device Users Through Image Selection,"* in Data Security, 2004.

[21] T. Takada and H. Koike, *"Awase-E: Image-based Authentication for Mobile Phones using Users Favorite Images,"* in Human-Computer Interaction with Mobile Devices and Services, vol. 2795/2003: Springer-Verlag GmbH, 2003, pp. 347-351.

[22] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, *"The Design and Analysis of Graphical Passwords,"* in Proceedings of the 8th USENIX Security Symposium, 1999.

[23] A. F. Syukri, E. Okamoto, and M. Mambo, *"A User Identification System Using Signature Written with Mouse,"* in Third Australasian Conference on Information Security and Privacy (ACISP): Springer- Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.

[24] G. E. Blonder, *"Graphical passwords,"* in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.

[25] L. D. Paulson, *"Taking a Graphical Approach to the Password,"* Computer, vol. 35, pp. 19, 2002.

[26] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, *"PassPoints: Design and longitudinal evaluation of a graphical password system,"* International Journal of Human Computer Studies, July 2005.

[27] Xiyang Liu, Jinhua Qiu, Licheng Ma, Haichang Gao, and Zhongjie Ren, *"A Novel Cued-recall Graphical Password Scheme."* Sixth International Conference on Image and Graphics, IEEE 978-0-7695-4541-7/11, 2011.

[28] J.C. Birget, D. Hong, and N. Memon, *"Robust discretization, with an application to graphical passwords,"* Cryptology ePrint archive 2003.

[29] Martin Mihajlov, Borka Jerman-Blazic and Marko Illievski. *"Recognition-based Graphical Authentication with Single-Object Images,"* Developments in E-systems Engineering, IEEE 2011.